2007

Mordell-Weil theorem and the rank of elliptical curves

Hazem Khalfallah

Mordell-Weil Theorem And The Rank Of Elliptic Curves

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Hazem Khalfallah

March 2007

Mordell-Weil Theorem And The Rank Of Elliptic Curves

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Hazem Khalfallah

March 2007

Approved by:

[redacted]
Dr. Ilseop Han, Committee Chair — Date 3/5/07

[redacted]
Dr. James Okon , Committee Member

[redacted]
Dr. Belisario Ventura, Committee Member

[redacted]
Dr. Peter Williams, Chair,
Department of Mathematics

[redacted]
Dr. Joseph Chavez
Graduate Coordinator,
Department of Mathematics

Abstract

An elliptic curve over a field is a nonsingular cubic curve in two variables with a rational point over the field. The set of these rational points forms an abelian group by the suitable definition of the group operation. If the field is an algebraic number field, Mordell-Weil theorem states that the group of rational points is finitely generated. The rank of an elliptic curve is the size of the smallest torsion-free generating set. The rank is very important in the study of elliptic curves. The rank is involved with many significant open questions on elliptic curves these days including the Birch and Swinnerton-Dyer Conjecture, which is one of the seven Millennium Prize problems established by the Clay Mathematics Institute. By using the proof of Mordell-Weil theorem, a formula for the rank of the elliptic curves in certain cases over algebraic number fields can be obtained and computable. This formula was first observed by J. Tate. The objective of this thesis is to give a detailed group theoretic proof of the rank formula in a more general setting and to give examples.

Acknowledgements

First, I want to thank God for giving me the intellect to explore the wonderful world of Mathematics. With his wisdom and courage, I am able to complete my thesis. I want to thank Dr. Ilseop Han for his great knowledge and help to overcome the difficulty of the topic. I want to thank my wife who was there for me. She is my inspiration and my forever friend. Lastly, I want to thank all the professors at California State University San Bernardino who helped me build strong mathematical foundation throughout the two years in the Master's program and prepared me to be successful in Mathematics.

Table of Contents

List of Figures

Chapter 1

Introduction

Let k be an algebraic number field, that is a finite field extension of $\mathbb{Q}$, the rational number field. Let $E(k)$ denote the group of rational points over k. Louis Mordell proved in 1922 that $E(\mathbb{Q})$ is finitely generated abelian group. This result was extended by Andre Weil in 1928 to abelian varieties over algebraic number field. Thus, $E(\mathbb{Q})$ has the following structure

$$E(k) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \quad times} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}.$$

The integer r, which is the size of the smallest torsion-free generating set, is called the rank of $E(k)$. It is obvious that $E(k)$ is finite if and only if $r = 0$.
Consider the elliptic curves

$$E : y^2 = x^3 + ax^2 + bx$$

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$$

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. The curves E and $\overline{E}$ have a close connection. There exist group homomorphisms

$$\phi : E \longrightarrow \overline{E} \qquad \text{and} \qquad \psi : \overline{E} \longrightarrow E$$

with the kernels of 2 elements: O the point at ∞ and $(0, 0)$. Further, the compositions $\psi \circ \phi$ and $\phi \circ \psi$ are multiplication by 2 and $\overline{\overline{E}} = E$.
Moreover, there exist group homomorphisms

$$\alpha : E(k) \longrightarrow k^*/k^{*2}$$

$$\begin{aligned} \alpha(O) &\longmapsto 1 \pmod{k^{*2}} \\ \alpha(T) &\longmapsto b \pmod{k^{*2}} \\ \alpha(x,y) &\longmapsto x \pmod{k^{*2}} \text{ if } x \neq 0 \end{aligned}$$

and

$$\overline{\alpha} : \overline{E}(k) \longrightarrow k^*/k^{*2}$$

Amazingly enough, $im(\alpha)$ (likewise $im(\overline{\alpha})$) is finite and computable. This also gives the formula for the rank of $E(k)$ (as well as $\overline{E}(k)$) as follows:

$$2^{r+2} = |im(\alpha)| \cdot |im(\overline{\alpha})|.$$

This formula is well-known and was first observed by John Tate. The purpose of this thesis is to give a detailed group theoretic proof of the rank formula in a more general setting and to give examples.

Chapter 2

Preliminary

In this chapter we will briefly review some important facts about curves. For more details see [ST92]. We know that a rational point is a quotient of two integers. We call a point in the (x, y) plane a *rational point* if both its coordinates are rational numbers. We call a *rational line* if the equation of the line can be written with rational number; that is, if its equation is

$$qx + py + t = 0$$

where q, p, t are rational. Now if we have two rational points, the line through them is a rational line. And if we have two rational lines, then the point where they intersect is a rational point. If we have two linear equations with a rational numbers as coefficients, and we solve them, we get rational numbers as answers.

2.1 The Geometry of Conic Curves

The general subject of this thesis is rational points on curves, especially on cubic curves. As an introduction we will start with conics. Let

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

be a conic. We will say that the conic is *rational* if we can write its equation with rational numbers. What about the intersection of rational conics and rational lines?
If we use analytic geometry to find the coordinates of these points, we will come out

with a quadratic equation for the x coordinate of the intersection that will have rational coefficients. Therefore, the two points of intersection will be rational if and only if the roots of the quadratic equation are rational. In general, they might be conjugate quadratic irrationalities. However, if one of those points is rational, then so is the other. Let α and β be two roots of the quadratic equation such that one of them is rational. So we can write the equation as

$$(x-\alpha)(x-\beta) = 0 \Rightarrow x^2 - (\alpha+\beta)x + \alpha \cdot \beta = 0.$$

The other root is rational because the sum of the roots is the middle coefficient. Given a rational conic, the first question is whether or not there is any rational points on it. Let us suppose that we know one of the rational point O is on our rational conic. We can get all of them by drawing a rational line and projecting the conic onto the line from this point O. To project O onto the line, we use the tangent line to the conic at O.
A line meets a conic in two points, so for every point Q on the conic we get a point P on the line; and conversely, for every point P on the line, by joining it to the point O, we get a point Q on the conic (Figure 2.1). Hence by the remarks we have made

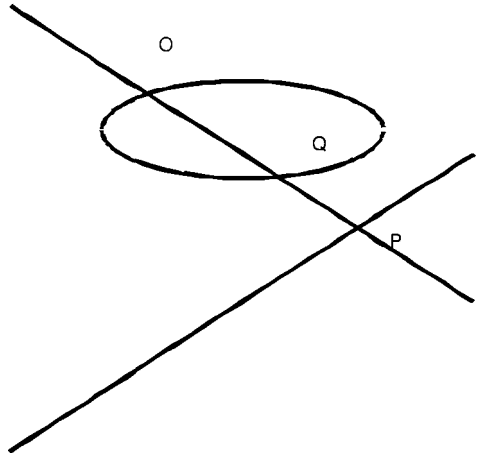


Figure 2.1: Projecting Conic Onto a Line

that if the point Q on the conic has rational coordinates, then the point P on the line

will have rational coordinates. Conversely, if P is rational, then because O is assumed to be rational, the line through P and Q meets the conic in two points, one of which is rational. Thus the other point is rational too. Therefore, the rational points on the conic are in one-to-one correspondence with the rational points on the line.
Note that the rational points on the line are easily described in terms of rational values of some parameter. Now what if we take the circle with radius $\sqrt{3}$ centred at the origin

$$x^2 + y^2 = 3$$

and ask to find the rational points on it? The answer is that there is none. It is impossible for the sum of the squares of two rational numbers to equal 3 or more generally $p \equiv 3 \pmod 4$. How can we see that it is impossible? From elementry number theory we have

2.1.1 Lemma

1. Let p be a prime

$$x^2 \equiv -1 \pmod p \text{ is solvable if and only if } p \equiv 1 \pmod 4$$

2. Let p be a prime

$$x^2 \equiv 2 \pmod p \text{ is solvable if and only if } p \equiv \pm 3 \pmod 8$$

Suppose there is a rational point, we can write it as

$$x = \frac{X}{Z} \qquad \textit{and} \qquad y = \frac{Y}{Z}$$

for some integers X, Y, Z and then

$$X^2 + Y^2 = pZ^2.$$

If X, Y, Z have a common factor, then we can remove it; so we may assume that they have no common factor. It follows that neither X nor Y is divisible by p, so we have

$$X^2 + Y^2 \equiv 0 \pmod p$$

together with

$$\gcd(X, p) = 1, \text{ and } \gcd(Y, p) = 1.$$

Without loss of generality if $\gcd(X,p) = 1$, then there exist X' such that $XX' = 1$. Therfore, we can say the following:

$$X'^2X^2 + X'^2Y^2 \equiv 0 \pmod{p}.$$

$$X'^2Y^2 \equiv -1 \pmod{p}.$$

By the previous lemma, this will be solvable if and only if $p \equiv 1 \pmod 4$. This shows that no two rational numbers have squares which add up to 3 (mod 4).

2.2 The Geometry of Cubic Curves

By definition elliptic curves are solutions of equations in two variables of degree three, with either y^3 or y^2 as a cubic function of x. Moreover, they are not elliptic in form and are called elliptic curve because their equation comes from computing the arc length of ellipse. Consider an ellipse centred at the origin as follows:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \qquad 0 < a \leq b.$$

In order to find the arc length say L of the entire ellipse, we will put

$$x = a\cos\theta, \qquad y = b\sin\theta, \qquad 0 \leq \theta \leq 2\pi$$

Then

$$L = \int_0^{2\pi} \sqrt{(\frac{dx}{d\theta})^2 + (\frac{dy}{d\theta})^2} \quad d\theta \tag{2.1}$$

$$= 4\int_0^{\frac{\pi}{2}} \sqrt{(-a\sin\theta)^2 + (b\cos\theta)^2} \quad d\theta \tag{2.2}$$

$$= 4b\int_0^{\frac{\pi}{2}} \sqrt{(\frac{a}{b})^2\sin^2\theta + \cos^2\theta} \quad d\theta \tag{2.3}$$

$$= 4b\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin^2\theta} \quad d\theta \quad k = \sqrt{1 - (\frac{a}{b})^2}. \tag{2.4}$$

Now if we let $u = \sin\theta$, then

$$du = \cos\theta d\theta = \sqrt{1 - \sin^2\theta} \quad d\theta = \sqrt{1 - u^2} \quad du \quad d\theta = \frac{du}{\sqrt{1 - u^2}}. \tag{2.5}$$

Hence

$$L = 4b\int_0^1 \frac{\sqrt{1 - k^2u^2}}{\sqrt{1 - u^2}} \quad du \tag{2.6}$$

$$L = 4b \int_0^1 \frac{1 - k^2u^2}{\sqrt{(1-u^2)(1-k^2u^2)}} \quad du. \tag{2.7}$$

Note that if the ellipse is not a circle (so, $0 < k < 1$), then the equation

$$v^2 = (1-u^2)(1-k^2u^2) \tag{2.8}$$

defines an elliptic curve. In fact, the equation (2.8) has four distinct roots and thus,

$$v^2 = (1-u)(1+u)(1-ku)(1+ku). \tag{2.9}$$

Dividing both sides by $(1-u)^4$, we have

$$\left(\frac{v^2}{(1-u)^2}\right)^2 = \frac{(1+u)(1-ku)(1+ku)}{(1-u)^3}$$

$$= \frac{(1-u+2u)}{(1-u)} \cdot \frac{(1-u+(1-k)u)}{(1-u)} \cdot \frac{(1-u+(1+k)u)}{(1-u)}$$

$$= \left(1+\frac{2u}{1-u}\right) \cdot \left(1+\frac{(1-k)u}{1-u}\right) \cdot \left(1+\frac{(1+k)u}{1-u}\right).$$

Putting $x = \frac{u}{1-u}$ and $y = \frac{v}{(1-u^2)}$, we have

$$y^2 = f(x) = (1+2x) \cdot (1+(1-k)x) \cdot (1+(1+k)x).$$

Note that f has three distinct roots and thus $y^2 = f(x)$ is an elliptic curve.

□

Let

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

be the equation for a general cubic. We will say that a cubic is rational if the coefficients of its equation are rational numbers. A famous example is:

$$x^3 + y^3 = 1;$$

or, in homogeneous form

$$X^3 + Y^3 = Z^3$$

To find rational solutions of $x^3+y^3 = 1$ amounts to finding integer solutions of $X^3+Y^3 = Z^3$, the first non-trivial case of Fermat's Last Theorem. If we find two rational points

on the elliptic curve, then we can find the third point. If we draw the line connecting the first two points we have a rational line that meets the cubic curve at the third point. If we intersect a rational line with a rational cubic we will have a cubic equation with rational coeffecients, and if the first two are rational the third will also be rational.
Recall that the goal is to reformulate Mordell's theorem in a way which has technical advantages. If we have any two rational points on a rational cubic, say P and Q, then we can draw the line joining P to Q obtaining the third point which we denoted $P * Q$. If we consider the set of all rational points on the cubic, we can say that set has a low of composition. Given any two points P, Q, we have defined a third point $P * Q$. We might ask about the algebraic structure of this set and this composition law; for example, is it a group?
Unfortunately, this is not a group because clearly there is no identity element. However, we can make it into a group in such a way that the given rational point O (the point at ∞) becomes the zero element of the group. We will denote the group law by $+$ because it is going to be a commutative group. The rule is as follows:

To add P and Q, take the third intersection point $P * Q$, join it to O, and then take the third intersection point to be $P + Q$. Thus by definition, $P + Q = O * (P * Q)$.

The group law is illustrated in figure 2.2. It is clear that this operation is commutative, that is, $P + Q = Q + P$. We first claim that $P + O = P$ and O acts as the zero element. Why is that? Well, if we join P to O, then we get the point $P * O$ as the third intersection point. The third intersection point is clearly P. Moreover, it is very obvious that the associative law holds and we have $(P + Q) * R = P * (Q + R)$ [ST92]
How does this allow us to reformulate Mordell-Weil Theorem? Mordell-Weil Theorem says that we can obtain all the rational points by starting with a finite set such as drawing lines through those points to get new points and then drawing lines through the new points to get more points and so on. In terms of the group law, this says that the group of rational points is finitely generated.

2.3 Weierstrass Normal Form

It is important to know that any cubic with a rational point can be transformed into a certain special form called *Weierstrass normal form*, which consist of equation that

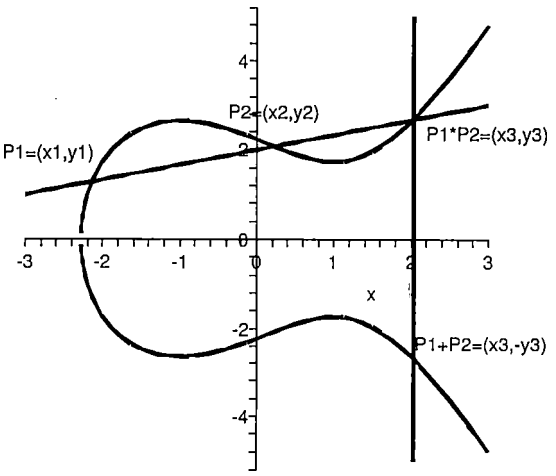


Figure 2.2: The Group Law on a Cubic

looks like the following:

$$y^2 = x^3 + ax^2 + bx + c,$$

Chapter 3

Nagell- Lutz Theorem

In order to characterize the groups of rational points on elliptic curves, we would like to be able to find elements of finite order in these groups. The Nagell-Lutz Theorem provides a way to determine if a point is of infinite order, therefore also allowing us, elimination, to determine the points of finite order.

3.1 Points of Order Two and Three

Let E be the non-singular cubic curve

$$E : y^2 = x^3 + ax^2 + bx + c$$

1. A point $P = (x, y) \neq O$ on E has order two if and only if $y = 0$.
2. E has exactly four points of order dividing two. These four points form a group which is a product of two cyclic groups of order two.
3. A point $P = (x, y) \neq O$ on E has order three if and only if x is a root of the polynomial [Kob93]

$$\phi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

4. E has exactly nine points of order dividing three. These nine points form a group which is a product of two cyclic groups of order three.

Besides points of order two and three, we have a very powerful theorem to help us narrow down our points.

3.1.1 Nagell-Lutz Theorem

Let

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c and let D be the discriminant of the cubic polynomial $f(x)$

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers and either $y = 0$, in which case P has order two , or y divides D.
Additionally, the strong form of The Nagell Lutz Theorem expands on this with the clarification that either $2P = O$ or y^2 divides the discriminant. The general direction of the proof of this theorem is straight forward.[ST92]

3.1.2 Example

We consider two examples showing the computation of the torsion subgroup T: Let $E : y^2 = x^3 + 4$. We see $D = -432$. Suppose $P = (x, y)$ is a point of finite order. Since $0 = x^3 + 4$ has no rational solutions, we must have $y \neq 0$. So by The Nagell - Lutz Theorem, we must have $y^2 | -432$. So the possibilities for y are

$$y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

Checking all of these, only $y = \pm 2$ give rational values for x, namely $x = 0$. So the only possible torsion points are $(0, 2)$ and $(0, -2)$. However, the criteria of point of order three states that a point $P = (x, y) \neq O$ on E has order three if and only if x is a root of the polynomial

$$\phi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

Checking our points $(0, \pm 2)$, both are roots of this equation.
A quick calculation shows that $3(0, \pm 2) = 0$. Since we have two rational points of order three together with our identity, the torsion subgroup will be $T \cong \mathbb{Z}/3\mathbb{Z}$.

Let

$$E : y^2 = x^3 + 8.$$

This time $D = -1728$ and if $y = 0$ then $x = -2$.

We know $(-2, 0)$ has order 2. Suppose $y \neq 0 \Longrightarrow y^2 | -1728 \Longrightarrow y | -24$. Checking all possibilities, only the points $(1, \pm 3)$ and $(2, \pm 4)$ satisfy E. However,

$$2(1,3) = \left(\tfrac{-7}{4}, \tfrac{-13}{8}\right) \qquad 2(2,4) = \left(\tfrac{-7}{4}, \tfrac{13}{8}\right)$$

Since these points do not have integer coordinates, they cannot have finite order. so $(1, \pm 3)$ and $(2, \pm 4)$ are not points of finite order either. Thus, the torsion subgroup of $E(Q)$ is $\{O, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$.

Chapter 4

The Mordell-Weil Theorem

In this section we will discuss Mordell-Weil Theorem in the case where at least one point of order 2 is rational, which say the subgroup $2E(k)$ has a finite index inside $E(k)$. where k is an algebraic number field . So we start by moving this point of order 2 to the origin, also we may assume that our elliptic curve is given by the equation[ST92]

$$E : y^2 = f(x) = x^3 + ax^2 + bx,$$

where a and b are integers. So

$$T = (0, 0)$$

is a rational point on E and satisfies $2T = O$.
The formula for the discriminant of f becomes in this case

$$D = b^2(a^2 - 4b).$$

We always assume our curve is non-singular which means that $D \neq 0$, and so neither $a^2 - 4b$ nor b is zero.
Since we are interested in the index $(E(k) : 2E(k))$, or the order of the factor group $E(k)/2E(k)$, it is extremely helpful to know that the duplication map $P \longmapsto 2P$ can be broken into two simpler operations.
The duplication map is of degree four because the rational function given the x coordinate of $2P$ is of order four in the x coordinate of P. So we will write the map $P \longmapsto 2P$ as a composition of two maps of degree two, each of which will be easier to handle. However,

the two maps will not be from E to itself, but rather from E to another curve $\overline{E}$ and then back again to E.

The other curve $\overline{E}$ that we will consider is the curve given by the equation

$$E : y^2 = x^3 + ax^2 + bx,$$

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where

$$\overline{a} = -2a \qquad and \qquad \overline{b} = a^2 - 4b.$$

These two curves are intimately related, and it is natural if you are studying E to also study $\overline{E}$. Now we are going to define a map $\phi : E \longmapsto \overline{E}$ which will be a group homomorphism and will carry the rational points $E(k)$ into the rational points $\overline{E}(k)$. And then by the same procedure we will define a map $\psi : \overline{E} \longmapsto E$. The composition $\psi \circ \phi$ is a homomorphism of E into E, which turn out to be a multiplication by 2. The map $\phi : E \longmapsto \overline{E}$ is defined in the following way:[ST92]

$$\phi(P) = (\tfrac{y^2}{x^2}, y(\tfrac{x^2-b}{x^2})), \qquad \text{if } P = (x, y) \neq O, T,$$

$$\overline{O}, \qquad \text{if } P = O \text{ or } P = T$$

The homomorphism ψ defined by

$$\psi(\overline{P}) = (\tfrac{\overline{y}^2}{4\overline{x}^2}, \tfrac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}), \qquad \text{if} \qquad \overline{P} = (\overline{x}, \overline{y}) \neq \overline{O}, \overline{T},$$

$$\psi(\overline{O}) = O, \qquad \psi(\overline{T}) = O$$

The composition $\psi \circ \phi : E \longrightarrow E$ is a multiplication by two:

$$\psi \circ \phi(P) = 2P.$$

Now we define a map $\alpha : E(k) \longrightarrow k^*/k^{*2}$. Recall that k^* is the multiplicative group of non-zero rational numbers, and let k^{*2} denote the subgroup of perfect squares. So k^*/k^{*2} is likely the nonzero rational numbers with two elements identified if their quotient is the square of rational number.

$$\alpha : E(k) \longrightarrow k^*/k^{*2}$$

$$\begin{aligned} \alpha(O) &\longmapsto 1 \pmod{k^{*2}} \\ \alpha(T) &\longmapsto b \pmod{k^{*2}} \\ \alpha(x,y) &\longmapsto x \pmod{k^{*2}}. \end{aligned}$$

The following proposition characterizes the behavior of α. For the proof of the following propositions, see [ST92]

4.1 Proposition 1

1. The map $\alpha : E(k) \longrightarrow k^*/k^{*2}$ is homomorphism groups.
2. The Kernel of α is $\phi(E(k))$, and α induces a natural injection
$$\frac{\overline{E}(k)}{\phi(E(k))} \hookrightarrow \frac{k^*}{k^{*2}}$$
3. Let $p_1, ..., p_r$ be the distinct primes dividing $\overline{b}$. Then the image of $\overline{\alpha}$ is contained in the subgroup of k^*/k^{*2} with representatives
$$\{(-1)^{\epsilon_0} p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_r^{\epsilon_r} \| \epsilon_i \in \{0,1\} i = 0, 1, ..., r\} \subset k^*/k^{*2}.$$
4. The index$[E(k) : \phi(E(k))]$ is finite .

4.2 Proposition 2

Let A and B be abelian groups with homomorphisms $\phi : A \longrightarrow B$ and $\psi : B \longrightarrow A$, such that

$$\psi \circ \phi(a) = 2a \text{ for all } a \in A \text{ and } \phi \circ \phi(b) = 2b \text{ for all } b \in B.$$

Also suppose that $[B : \phi(A)]$ and $[A : \phi(B)]$ are finite.

Then the index $[A : 2A]$ is finite.

4.3 The Mordell-Weil Theorem

For curves with a rational point of order two. Let E be a non-singular cubic curve given by an equation

$$E : y^2 = x^3 + ax^2 + bx,$$

where a and b are integers. Then the group of rational point $E(k)$ is a finitely generated abelian group. Mordell's theorem tells us that we can produce all of the rational points on E by starting from finite set and using geometry. The proof of Mordell's theorem gives us some tools, but the next section is more interesting which is the heart of this paper.

Chapter 5

Computing The Rank of Elliptic Curves

Mordell's theorem tells us that the group of rational points $E(k)$ on the curve

$$E : y^2 = x^3 + ax^2 + bx,$$

is a finitely generated abelian group. It follows from the fundamental theorem on abelian groups that $E(k)$ is isomorphic as an abstract group, to a direct sum of infinite cyclic groups and finite cyclic groups of prime power order.

We will let $\mathbb{Z}$ denote the additive group of integers, and we will let $\mathbb{Z}m$ denote the cyclic group $\mathbb{Z}/m\mathbb{Z}$ of integers mod m. Then the structure of $E(k)$ will look like the following

$$E(\mathbb{K}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \quad times} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}.$$

This means that there is generators

$$P_1, ...P_r, Q_1, ..., Q_s \in E(k)$$

such that every $P \in E(k)$ can be written in the form

$$P = n_1P_1 + ... + n_rP_r + m_1Q_1 + ... + m_sQ_s.$$

The integer r is called the rank of $E(k)$. The group $E(k)$ will be finite if and only if it has rank $r = 0$. The subgroup

$$\mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}.$$

corresponds to the elements of finite order in $E(K)$ it has order $p_1^{v_1}, p_2^{v_2}, ..., p_s^{v_s}$. Of course, the points $P_1, ..., P_r, Q_1, ..., Q_s$ are not unique, so there are too many choices of generators for $E(k)$.

Computing the rank of an elliptic curve is harder than computing the elements of finite order in $E(k)$. The proof of Mordell's Theorem allows us to determine the quotient group $E(k)/2E(k)$[ST92]

$$E(k) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \quad times} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}.$$

$$2E(k) \cong \underbrace{2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{r \quad times} \oplus 2\mathbb{Z}_{p_1^{v_1}} \oplus 2\mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus 2\mathbb{Z}_{p_s^{v_s}}$$

$$\frac{E(k)}{2E(k)} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}}_{r \quad times} \oplus \frac{\mathbb{Z}_{p_1^{v_1}}}{2\mathbb{Z}_{p_1^{v_1}}} \oplus ... \oplus \frac{\mathbb{Z}_{p_s^{v_s}}}{2\mathbb{Z}_{p_s^{v_s}}}$$

Now $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ is cyclic of order two, whereas

$$\frac{\mathbb{Z}_{p_s^{v_s}}}{2\mathbb{Z}_{p_s^{v_s}}} \cong \mathbb{Z}_2, \qquad if \qquad p_i = 2$$

$$\frac{\mathbb{Z}_{p_s^{v_s}}}{2\mathbb{Z}_{p_s^{v_s}}} \cong 0, \qquad if \qquad p_i \neq 2$$

Therefore,

$$(E(k) : 2E(k)) = 2^{r+(number of j with p_j=2)}$$

$$\text{let } \tau = \text{ (number of j with} p_j = 2).$$

Now to ease the notation let $E(k) = G$, $2E(k) = 2G$, $\overline{E}(k) = G'$, and let G_2 denote the subgroup of all $k \in G$ such that $2k = O$. How this group look like?

$$2(n_1P_1 + ... + n_rP_r + m_1Q_1 + ... + m_sQ_s) = 0.$$

This happen if $n_i = 0$ for each i, and $2m_j \equiv 0 \pmod{p_j^{v_j}}$. Now if p is odd and $2m \equiv 0 \pmod{p^v}$, then $m \equiv 0 \pmod{p^v}$. Now if $p = 2$, and $2m \equiv 0 \pmod{p^v}$, then we conclude that $m \equiv 0 \pmod{p^{v-1}}$. So the order of the new subgroup G_2 is

$$|G_2| = 2^{(number of j with p_j=2)} = 2^{\tau}$$

Combining these two formulas, we obtain the useful result:[ST92]

$$(G : 2G) = 2^r \cdot |G_2| = 2^{r+\tau}$$

This formula holds for any finitely generated abelian group of rank r. So we have

$$|G_2| = 2^{(numberofjwithp_j=2)} = 2^\tau, \text{ and } G_2 = O \cup \{P(x,y) \in G | y = 0\}.$$

Since the equation $f(x) = 0$ has at most three integer roots, we find that $|G_2| \leq 4$. G_2 contains at least the elements O and $T(0,0)$ of G and its order is a power of two least or equal to 4, hence $|G_2| \in \{2, 4\}$.

If $|G_2| = 4$ if and only if there are three points of order 2. So the equation $f(x) = 0$ has three integer solutions and $a^2 - 4b = c^2$ for some integer c.

5.1 Modules

5.1.1 Definition

Let R be a commutative ring with an identity element 1_R. Recall that $R-$module is an additive abelian group M together with a mapping

$$R \times A \longrightarrow A$$

$$(r, a) \longmapsto r \cdot a$$

such that for all $r, s \in R$ and $a, b \in A$

1. $r(a+b) = ra + rb$
2. $(r+s)a = ra + sa$
3. $r(sa) = (rs)a$
4. $1_R a = a$ for all $a \in A$.

Since we assume that R is commutative, we have $ra = ar$ for any $r \in R$ and $a \in A$. Note that if R is a field, then A is a vector space over R. Moreover, every additive abelian group is a $\mathbb{Z}-$module. Since the group $E(k)$ of rational points over a field k forms an abelian group, so a $\mathbb{Z}-$module. We will briefly review some important facts on $R-$module.

Let A and B are $R-$modules. A map $f : A \to B$ is an $R-$module homomorphism, or simply $R-$map if

$$f(a+b) = f(a) + f(b)$$

$$f(ra) = rf(a)$$

for any $a, b \in A$, and $r \in R$. If R is a field, then an $R-$module homomorphism is called a linear transformation.

Now consider a sequence of $R-$module homomorphism

$$\cdots \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} \cdots$$

We say that the sequence is exact at B if $im(f) = ker(g)$. If this is the case at every $R-$module, then we say the sequence is exact.

Note then that

1. A $R-$map $A \xrightarrow{f} B$ is injective if and only if $O \longrightarrow A \xrightarrow{f} B$ is exact.

2. A $R-$map $B \xrightarrow{g} C$ is surjective if and only if $B \xrightarrow{g} C \longrightarrow O$ is exact.

3. If $A \xrightarrow{f} B \xrightarrow{g} C$ is exact, then $g \circ f$ is a zero map.

4. From a A $R-$map $A \xrightarrow{f} B$, there exists a exact sequence
   $O \longrightarrow ker(f) \longrightarrow A \xrightarrow{f} B \longrightarrow coker(f) \longrightarrow O$, where $coker(f) = B/im(f)$.

5. $O \longrightarrow A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \longrightarrow O$ is exact, where the map i and π are the canonical injection and projection respectively where $\oplus$ is the direct sum.

For the following lemma see[Sur00]

5.2 Snake Lemma

Let R be a commutative ring with 1_R. Suppose there exist a commutative diagram of $R-$modules with exact rows

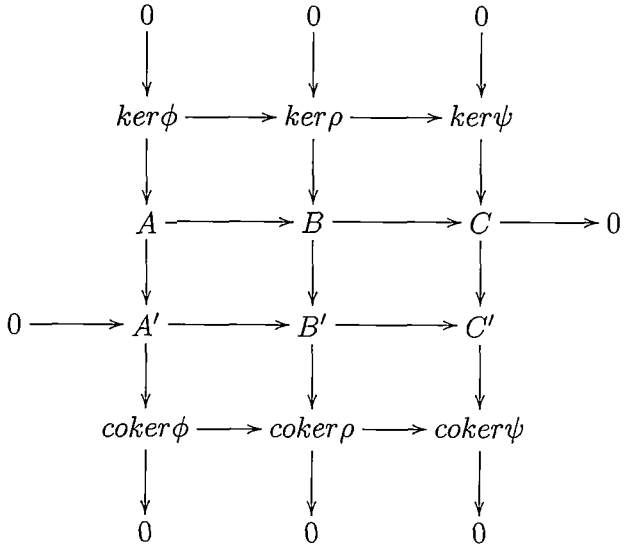
$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C \longrightarrow 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \psi} \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

Then there exist a map $\delta : ker(\psi) \rightarrow coker(\phi)$ and the sequence

$$ker(\phi) \longrightarrow ker(\rho) \longrightarrow ker(\psi) \xrightarrow{\delta} coker(\phi) \longrightarrow coker(\rho) \longrightarrow coker(\psi)$$

is exact. Furthermore, if f is injective, then so is the map $ker(\phi) \longrightarrow ker(\rho)$, and if g' is surjective, then so is $coker(\rho) \longrightarrow coker(\psi)$.

The name of this lemma derives from the following commutative diagram with exact rows, and exact columns.



5.2.1 Proposition 3

Let R be a commutative ring with 1_R.
For any pair of maps $A \xrightarrow{f} B \xrightarrow{g} C$, of R–modules, there is an exact sequence

$$0 \longrightarrow ker f \longrightarrow ker(g \circ f) \longrightarrow ker g \longrightarrow coker f \longrightarrow coker(g \circ f) \longrightarrow coker g \longrightarrow 0 \tag{5.1}$$

5.2.2 Proof

There is a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \oplus B & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g \circ f} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & B & \longrightarrow & C \oplus B & \longrightarrow & C & \longrightarrow & 0 \end{array} \tag{5.2}$$

Note that the middle vertical map is component wisely the composition $g \circ f : A \longrightarrow C$ together with the identity map $i : B \longrightarrow B$. Hence, we may identify $(g \circ f, i)$ with $g \circ f$.

Now we apply the snake Lemma to the diagram (5.2), and obtain the exact sequence (5.1).

□

The following is a different alternative proof for the exactness of abelian group

5.2.3 Alternative Proof (Exactness of Abelian Group)

For any pair of maps $A \xrightarrow{f} B \xrightarrow{g} C$ of abelian groups there is an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & ker(f) & \longrightarrow & ker(g \circ f) & \xrightarrow{\bar{f}} & ker(g) & & \\ & & & & & & \downarrow \phi & & \\ & & & & & & coker(f) & \xrightarrow{\bar{g}} & coker(g \circ f) \longrightarrow coker(g) \longrightarrow 0 \end{array}$$

5.2.4 Proposition 4

Consider the homomorphism $\bar{f} : ker(g \circ f) \longrightarrow ker(g)$ by $a \longrightarrow f(a)$. This is well defined, if $a \in ker(g \circ f)$, then $f(a) \in ker(g)$. Clearly $ker(\bar{f}) = \ker(f)$.
Hence we get an exact sequence

$$0 \longrightarrow ker(f) \longrightarrow ker(g \circ f) \longrightarrow ker(g).$$

Similarly, consider the homomorphism $\bar{g} : coker(f) \longrightarrow coker(g \circ f)$ by $b + imf \longmapsto g(b) + im(g \circ f)$. This is again well defined and provides us with exact sequence

$$coker(f) \longrightarrow coker(g \circ f) \longrightarrow coker(\bar{g}) \longrightarrow 0.$$

We can glue these sequences together in the following way:
we need to define a homomorphism $\phi : ker(g) \rightarrow coker(f)$ by $\phi(b) = b + im(f)$, then

$$ker(\phi) = ker(g \cap im(f)) = f(ker(g \circ f)) = im(\bar{f}).$$

So $im(\phi) = ker(\bar{g})$. In fact, $im(\phi)$ is the subgroup of $B/im(f)$ whose cosets are represented by elements in the kernel of g, hence $im(\phi) \subseteq ker(\bar{g})$.
On the other hand, $b + im(f) \in ker(\bar{g})$ is equivalent to $g(b) \in im(g \circ f)$, which holds if and only if b can be written in the form $b = b' + f(a)$, for some $b' \in ker(g)$. But

this implies $b + im(f) \in im(\phi)$. The claim now follows from the simple observation that $coker(\overline{g}) = coker(g)$. In fact, the map

$$coker(g \circ f) \longmapsto coker(g)$$
$$c + im(g \circ f) \longrightarrow c + im(g)$$

is surjective and the kernel consist of all the elements of the form $f(b) + im(g \circ f)$ and so the kernel is $im\bar{g}$. so we will glue it this way

$$\begin{array}{ccccccccc} 0 & \longrightarrow & ker(f) & \longrightarrow & ker(g \circ f) & \longrightarrow & ker(g) & & \\ & & & & & & \downarrow & & \\ & & & & & & coker(f) & \longrightarrow & coker(g \circ f) \longrightarrow coker(g) \longrightarrow 0 \end{array}$$

5.2.5 Lemma 3

Let R be a commutative ring with 1_R. If the sequence

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow ... \longrightarrow A_n \longrightarrow 0$$

of finite $R-$modules is exact, then

$$\frac{|A_1| \cdot |A_3| \cdot |A_5| \cdot \cdot}{|A_2| \cdot |A_4| \cdot |A_6| \cdot \cdot} = 1$$

5.2.6 Proof

This is easly proved by induction. If

$$0 \longrightarrow A_1 \longrightarrow 0$$

is exact, it is obvious that $|A_1| = 1$. And if

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow 0$$

is exact, then $A_1 \cong A_2$, and $\frac{|A_1|}{|A_2|} = 1$.
Now suppose that

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow ... \longrightarrow A_n \longrightarrow A_{n+1} \longrightarrow 0$$

is exact, note then that

$$0 \longrightarrow A_2/A_1 \longrightarrow A_3 \longrightarrow ...A_{n+1} \longrightarrow 0$$

is exact. By induction hypothesis, we have

$$\frac{|A_2/A_1| \cdot |A_4| \cdot |A_6| \cdot \cdot}{|A_3| \cdot |A_5| \cdot |A_7| \cdot \cdot} = 1$$

or

$$\frac{|A_2| \cdot |A_4| \cdot |A_6| \cdot \cdot}{|A_1| \cdot |A_3| \cdot |A_5| \cdot \cdot} = 1$$

□

5.2.7 Proposition 5

Let R be a commutative ring with 1_R. For any pair of maps $A \xrightarrow{f} B \xrightarrow{g} C$, of finite $R-$modules, we have

$$\frac{|coker(g \circ f)|}{|ker(g \circ f)|} = \frac{|coker(g)||coker(f)|}{|ker(g)||ker(f)|} \tag{5.3}$$

5.2.8 Proof

By proposition 3 and Lemma 3, we have

$$|coker(g \circ f)||ker(g)||ker(f)| = |coker(g)||coker(f)||ker(g \circ f)| \tag{5.4}$$

Rewriting this equality, we have

$$\frac{|coker(g \circ f)|}{|ker(g \circ f)|} = \frac{|coker(g)||coker(f)|}{|ker(g)||ker(f)|}$$

□

5.3 The Rank of Elliptic Curve

Let k be an algebraic number field, then by Mordell-Weil Theorem, $E(k)$ is a finitely generated abelian group (so $\mathbb{Z}$-module). Now we have to recall the maps of the last steps of Mordell-Weil Theorem ϕ, ψ, α and $\overline{\alpha}$.

$$E(k) \xrightarrow{\phi} \overline{E}(k) \xrightarrow{\psi} E(k).$$

Proposition 3 then gives us the exact sequence

$$0 \longrightarrow ker(\phi) \longrightarrow ker(\psi \circ \phi) \longrightarrow ker(\psi)$$
$$\downarrow$$
$$coker(\phi) \longrightarrow coker(\psi \circ \phi) \longrightarrow coker(\psi) \longrightarrow 0$$

Now $ker(\phi) = \{O, T\}, ker(\psi \circ \phi) = E(k)_2, ker(\psi) = \{\overline{O}, \overline{T}\}, coker(\psi) = \overline{E}/im(\phi) \cong \overline{E}/ker(\overline{\alpha}) \cong im(\overline{\alpha}), coker(\psi \circ \phi) = \overline{E}(k)/2\overline{E}(k)$ and $coker(\psi) \cong E/ker(\alpha) \cong im(\alpha)$.
So the above exact sequence become

$$0 \longrightarrow \{O, T\} \longrightarrow E(\mathbb{Q})_2 \longrightarrow \{\overline{O}, \overline{T}\}$$
$$\downarrow$$
$$im(\overline{\alpha}) \longrightarrow E(k)/2E(k) \longrightarrow im(\alpha) \longrightarrow 0$$

If we put $|E(k)_2| = 2^\tau$, then since $E(k)$ is finitely generated,and Mordell's theorem proved that $(E(k) : 2E(k)) = (G : 2G) = 2^{r+\tau}$, now applying lemma 3

$$\frac{\|ker(\phi)||ker(\psi)||coker(\psi \circ \phi)|}{|ker(\psi \circ \phi)||coker(\phi)||coker(\psi)|} = 1$$

$$|ker(\phi)||ker(\psi)||coker(\psi \circ \phi)| = |ker(\psi \circ \phi)||coker(\phi)||coker(\psi)|$$

$$|\{O, T\}| \cdot |\{O, \overline{T}\}| \cdot |E(k)/2E(k)| = |E(k)[2]| \cdot |im(\overline{\alpha})| \cdot |im(\alpha)|$$

$$2 \cdot 2 \cdot 2^{r+\tau} = 2^\tau \cdot |im(\alpha)| \cdot |im(\overline{\alpha})|$$

Hence, we finally have:

5.3.1 Proposition 6

Let E and E' be elliptic curves and α and α' be maps as before. If r is the rank of E, then

$$2^r = \frac{|im(\alpha)| \cdot |im(\overline{\alpha})|}{4}$$

It is this formula we will use to compute the rank.

Chapter 6

Examples

Let E be an elliptic curve over $\mathbb{Q}$ with the form

$$E : y^2 = x^3 + ax^2 + bx.$$

Then it is known [ST92] that the coordinates of rational point (x, y) on E have the form

$$x = \frac{m}{e^2}, \qquad y = \frac{n}{e^3},$$

where $m, n, e, \in \mathbb{Z}$ in lowest terms with $e > 0$,with $gcd(m, e) = gcd(n, e) = 1$. Let $n \neq 0$ (and so $m \neq 0$), then

$$(\frac{n}{e^3})^3 = (\frac{m}{e^2})^3 + a(\frac{m}{e^2})^2 + b((\frac{m}{e^2})$$

or

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$

Let $b_1 = \pm gcd(m, b)$, where $mb_1 > 0$. Then we can write

$$m = b_1m_1 =, \qquad b = b_1b_2, \quad \text{with } gcd(m_1, b_2) = 1 \text{ and } m_1 > 0 \text{ for some } m_1, b_2 \in \mathbb{Z}$$

If we substitute in the equation of the curve, we get

$$n^2 = b_1m_1(b_1^2m_1^2 + ab_1m_1e^2 + b_1b_2e^4) = b_1^2m_1(b_1m_1^2 + am_1e^2 + b_2e^4).$$

This tells us that, $b_1^2|n^2$, so $b_1|n$ and we can write $n = b_1n_1$. Hence,

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4).$$

Since $gcd(b_2, m_1) = gcd(e, m_1) = 1$, we see that the $gcd(m_1, b_1 m_1^2 + a m_1 e^2 + b_2 e^4) = 1$. So we may assume that each of them is square. Hence we can factor n_1 as $n_1 = MN$ so that

$$M^2 = m_1 \qquad N^2 = b_1 m_1^2 + a m_1 e^2 + b_2 e^4.$$

substitute $M^2 = m_1$ into the second equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4.$$

Hence

$$x = \frac{b_1 M^2}{e^2}, \qquad y = \frac{b_1 MN}{e^3}$$

where

$$\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = 1 \gcd(b_2, M) = \gcd(M, N) = 1 \text{ ; [ST92]}$$

Replacing (x, y) by $(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3})$ on the equation of E, we have

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4..$$

Note that any solution to this equation gives a rational point on E.

6.1 Example 1

In our first example, let p be a prime number with $p \equiv 3 \pmod 8$.
consider the elliptic curve:

$$E : y^2 = x^3 - px,$$

For the map $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$, we have $\{\overline{1}, -\overline{p}\} \subseteq im(\alpha)$, where $\overline{x}$ means $x \pmod{\mathbb{Q}^{*2}}$.
The equations to consider are

$$N^2 = M^4 - pe^4, \qquad [a]$$

$$N^2 = -M^4 + pe^4, \qquad [b]$$

$$N^2 = pM^4 - e^4, \qquad [c]$$

$$N^2 = -pM^4 + e^4, \qquad [d]$$

we have $b_1 \cdot b_2 = -p$, so it is clear that $b_1 = 1$ and $b_2 = -p \in im(\alpha)$. From the symetry, it suffices to consider only one equation [b] or [c].

$$N^2 = -M^4 + pe^4 \qquad N^2 \equiv -M^4 \pmod p$$

Note that$M \neq 0 \pmod p$. Otherwise, $N \equiv 0 \pmod p$ and so $gcd(M, N) \neq 1$ which is absurd.

$$\frac{N^2}{M^4} \equiv -1 \pmod p \qquad (\frac{N}{M^2})^2 \equiv -1 \pmod p$$

Now we recall Lemma 1, this equation has no solution $\pmod p$ where $p \equiv 3 \pmod 4$.Hence, we can conclude that $im(\alpha) = \{1, -p\}$.
Consider the curve

$$\overline{E} : y^2 = x^3 + 4px.$$

For the map $\overline{\alpha} : \overline{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$, we have $\{\overline{1}, \overline{p}\} \subseteq im(\overline{\alpha})$. Since $\overline{b} = a^2 - 4b = 4p$, the possibilities for $\overline{b_1}$ are

$$\overline{b_1} = \pm 1, \pm 2, \pm 4, \pm p, \pm 2p, \pm 4p$$

But $\pm 4 = \pm(2^2)$ and $\pm 4p = \pm(2^2) \cdot p$, so the possibilities for $\overline{b_1}$ modulo square are

$$\overline{b_1} = \pm 1, \pm 2, \pm p, \pm 2p$$

However, both factors of $4p$ can not be negative since$N^2 > 0$.The equations to consider are

$$N^2 = M^4 + 4pe^4, \qquad [a']$$

$$N^2 = 2M^4 + 2pe^4, \qquad [b']$$

$$N^2 = pM^4 + 4e^4, \qquad [c']$$

$$N^2 = 2pM^4 + 2e^4, \qquad [d']$$

Since $\{\overline{1}, \overline{p}\} \subseteq im(\overline{\alpha})$ and the symetry of [b'] and [c'], it suffices to consider [b'] only.

$$X^2 = 2Y^4 + 2pe^4 \qquad X^2 \equiv 2Y^4 \pmod{p} \qquad \frac{X^2}{Y^4} \equiv 2 \pmod{p}$$

$$(\frac{X}{Y^2})^2 \equiv 2 \pmod{p}$$

Now we recall Lemma 2, this equation $(\frac{X}{Y^2})^2 \equiv 2 \pmod{p}$ has no solution $\pmod{p}$ where $p \equiv 3 \pmod{4}$.Hence, we can conclude that $im(\overline{\alpha}) = \{\overline{1}, \overline{p}\}$.
Putting all this together, we find that

$$2^r = \frac{|im(\alpha)| \cdot |im(\overline{\alpha})|}{4} = \frac{2 \cdot 2}{4} = 1 \Rightarrow r = 0$$

So the rank of $E(\mathbb{Q}))$ is 0, as is the rank of $\overline{E}(\mathbb{Q})$. This shows that the group of rational points on E and $\overline{E}$ are each finite, and so all the rational points have finite order.
Let p be a prime number. The only points of finite order on the curve $E : y^2 = x^3 - px$ are O and $(0, 0)$.[ST92]

$$P \in E(\mathbb{Q}) : \text{P has finite order} \cong \begin{cases} \frac{\mathbb{Z}}{4\mathbb{Z}} & \text{if } D = 4d^4 \text{ for some d,} \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} & \text{if } D = -d^2 \text{ for some d,} \\ \frac{\mathbb{Z}}{2\mathbb{Z}} & \text{otherwise} \end{cases}$$

6.2 Example 2

We consider the two curves:

$$E : y^2 = x^3 + 3x^2 + 5x, [1] \qquad \overline{E} : y^2 = x^3 - 6x^2 - 11x, \qquad [2]$$

For the map $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$, we have $\{\overline{1}, \overline{5}\} \subseteq im(\alpha)$. For the curve E, we have $a = 3$ and $b = 5$, so the possibilities for b_1 are $\pm 1, \pm 5$ and b_2 are $\pm 1, \pm 5$,and $b_1 \cdot b2 = 5$. The equations to consider are

$$N^2 = M^4 + 3M^2e^2 + 5e^4, \qquad [3]$$

$$N^2 = -M^4 + 3M^2e^2 - 5e^4, \qquad [4]$$

$$N^2 = 5M^4 + 3M^2e^2 + e^4, \qquad [5]$$

$$N^2 = -5M^4 + 3M^2e^2 - e^4, \qquad [6]$$

Note that [3] and [4] are the same as [5] and [6] respectively, with the variables M and e reversed. Since the solutions that we will find satisfy $Me \neq 0$, it is enough to consider the first two equations. After trial and error we see that $(M, e, N) = (1, 1, 3)$ is a solution to [3],since

$$3^2 = (1)^4 + 3 \cdot 1^2 \cdot 1^2 + 5 \cdot 1^4.$$

We need to show that [4] and [6] have no solutions in integers. First we will calculate the discriminant D.

$$D = b^2(a^2 - 4b) = 25 \cdot (9 - 20) = -275 = -5^2 \cdot 11.$$

Note that if [4] (as well as [6]) is solvable, then so is the equation modulo 11. However, the set solution for the left hand side is $L = \{0, 1, 3, 4, 5, 9\}$, and for the right hand side is $R = \{2, 6, 8, 10\}$. It is obvious that $L \cap R$ is the empty set, which means that the equation is not solvable (mod 11). Hence both equations [4] and [6] has no solutions in integers. So we conclude that $im(\alpha)$ has order 2.

Now for the second equation

$$\overline{E} : y^2 = x^3 - 6x^2 - 11x,$$

we have $a = -6$ and $b = -11$, so the possibilities for b_1 are $\pm 1, \pm 11$ and b_2 are $\pm 1, \pm 11$ and $b_1 \cdot b2 = -11$.

$$\overline{\alpha} : \overline{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

$$\begin{aligned} \overline{\alpha}(O) &\longmapsto 1 \pmod{\mathbb{Q}^{*2}} \\ \overline{\alpha}(0,0) &\longmapsto -11 \pmod{\mathbb{Q}^{*2}} \\ \overline{\alpha}(x,y) &\longmapsto x \pmod{\mathbb{Q}^{*2}}. \end{aligned}$$

Hence, $\{\overline{1}, \overline{-11}\} \subseteq im(\overline{\alpha})$ and the equations to consider are

$$N^2 = M^4 - 6M^2e^2 - 11e^4, \qquad [7]$$

$$N^2 = -M^4 - 6M^2e^2 + 11e^4, \qquad [8]$$

$$N^2 = -11M^4 - 6M^2e^2 + e^4, \qquad [9]$$

$$N^2 = 11M^4 + 3M^2e^2 - e^4, \qquad [10]$$

Note that [7] and [8] are the same as [9] and [10] respectively, with the variables M and e reversed. Since the solutions that we will find satisfy $Me \neq 0$, it is enough to consider the first two equations. So after trial and error we see that $(M, e, N) = (3, 1, 4)$ is a solution to [7], since

$$4^2 = (1)^4 - 6 \cdot 3^2 \cdot 1^2 - 11 \cdot 1^4.$$

Also (1,1,2) is a solution for [8] and [10], since

$$2^2 = -(1)^4 - 6 \cdot 1^2 \cdot 1^2 + 11 \cdot 1^4.$$

So we conclude that $im(\overline{\alpha})$ has order 4. Putting all this together, we find that

$$2^r = \frac{|im(\alpha)| \cdot |im(\overline{\alpha})|}{4} = \frac{2 \cdot 4}{4} = 2 \Rightarrow r = 1$$

Which means the rank of $E(\mathbb{Q})$ is 1. Hence E has an infinite number of rational points.

6.3 Example 3

We consider the two curves

$$E : y^2 = x^3 - 17x, [1] \qquad \overline{E} : y^2 = x^3 + 68x, \qquad [2]$$

Recall that our general elliptic curve is represented by the equation $y^2 = x^3 + ax^2 + bx$, so in [2], we have $a = 0$ and $b = 68$. For the curve E, we have $a = 0$ and $b = -17$, so the possibilities for b_1 are $\pm 1, \pm 5$.

$$\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

$$\begin{aligned} \alpha(O) &\longmapsto 1 \pmod{\mathbb{Q}^{*2}} \\ \alpha(0,0) &\longmapsto -17 \pmod{\mathbb{Q}^{*2}} \\ \alpha(x,y) &\longmapsto x \pmod{\mathbb{Q}^{*2}}. \end{aligned}$$

we have $\{\overline{1}, -17\} \subseteq im(\alpha)$, and the equations to consider are

$$N^2 = M^4 - 17e^4, \qquad [a]$$

$$N^2 = -M^4 + 17e^4, \qquad [b]$$

$$N^2 = 17M^4 - 1e^4, \qquad [c]$$

$$N^2 = -17M^4 + e^4, \qquad [d]$$

Note that [a] and [b] are the same as [d] and [c] respectively, with the variables M and e reversed. Since the solutions that we will find satisfy $Me \neq 0$, it is enough to consider the first two equations. So after trial and error we see that $(M, e, N) = (1, 1, 4)$ is a solution to [b], since

$$4^2 = -(1)^4 + 17 \cdot 1^4.$$

Also$(M, e, N) = (4, 2, 4)$ is a solution to [b]

$$4^2 = -(4)^4 + 17 \cdot 2^4.$$

So all four equation [a]-[d] have solutions and we can use the formulas

$$x = \frac{b_1 M^2}{e^2}, \qquad y = \frac{b_1 NM}{e^3}.$$

to find the following rationals points on E:

$$(b_1, Y, e, N) = (-1, 1, 1, 4) \Rightarrow x = -1 \quad and \quad y = 4$$

$$(b_1, M, e, N) = (-17, 1, 1, 4) \Rightarrow x = 17 \quad and \quad y = 68;$$

$$(b_1, M, e, N) = (-1, 4, 2, 4) \Rightarrow x = -4 \quad and \quad y = 2;$$

$$(b_1, M, e, N) = (17, 2, 4, 4) \Rightarrow x = 17/4 \quad and \quad y = 17/8.$$

This proves that $E(\mathbb{Q}) = \{\pm 1, \pm 17\} \pmod{\mathbb{Q}^{*2}}$, which is the Klein four Group. So the order of $\alpha(E) = 4$.
For$\overline{\alpha}$ we have $\overline{b} = a^2 - 4b = 68$, the possibilities for $\overline{b_1}$ are

$$\overline{b_1} = \pm 1, \pm 2, \pm 4, \pm 17, \pm 34, \pm 68.$$

But $\pm 4 = \pm(2^2)$ and $\pm 68 = \pm(2^2) \cdot 17$, so the possibilities for $\overline{b_1}$ modulo square are

$$\overline{b_1} = 1, 2, 17, 34$$

We know that $\overline{\alpha}(\overline{O}) = 1$ and $\overline{\alpha}(\overline{T}) = \overline{b} = 68 \equiv 17 \pmod{\mathbb{Q}^{*2}}$ are both in $\overline{\alpha}(\overline{E}(\mathbb{Q}))$. We shall next show that $\overline{b}_1 = 2$ and $\overline{b}_2 = 34$ are both in $im(\overline{\alpha})$. We need to check if the equation

$$N^2 = 2M^4 + 34e^4 \qquad [f]$$

has a solution in integers, and after trial and error we see that $(M, e, N) = (3, 1, 14)$ is a solution to [f], since

$$14^2 = 2 \cdot 3^4 + 34 \cdot 1^4.$$

Last we know $2 \in \overline{\alpha}(E)$ then $34 = 2*17 \in \overline{\alpha}(E)$ and the order of $\overline{\alpha}(E) = 4$. Putting all this together, we find that

$$2^r = \frac{|im(\alpha)| \cdot |im(\overline{\alpha})|}{4} = \frac{4 \cdot 4}{4} = 4 \Rightarrow r = 2$$

Which means the rank of $E(\mathbb{Q})$ is 2. Hence E has an infinite number of rational points.

The current record for the rank of elliptic curve is 28, found by Elkies in 2006, and the previous record was 24, found by Martin and McMillen in 2000. The following table shows the values of the rank r for E given by $y^2 = x^3 + ax$.

rank r	values of a
r=0	a = 1, 2, 4, 6, 7, 10, 11, 12, 22, -1, -3, -4, -8, -9, -11, -13, -18, -19
r=1	a = 3, 5, 8, 9, 13, 15, 18, 19, 20, -2, -5, -6, -7, -10, -12, -14, -15, -20
r=2	a = 14, 33, 34, 39, 46, -17, -56, -65, -77
r=3	a = -82

Table 6.1: Values of the rank r for E given by $y^2 = x^3 + ax$

Bibliography

[BSD65] B. Birch and H. P. F. Swinnerton-Dyer. *Notes on elliptic curves 2.* Undergraduate Texts in Mathematics. 1965.

[Bur89] David M. Burton. *Elementary number theory.* W. C. Brown Publishers, Dubuque, IA, second edition, 1989.

[GS95] Robert Gross and Joseph Silverman. S-integer points on elliptic curves. *Pacific J. Math.*, 167(2):263–288, 1995.

[HHD02] Wadsworth.A Han.I Haile HHD. Relative brauer groups of function fields of curves of genus one. (1), 2002. Preprint.

[Kna92] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes.* Princeton University Press, Princeton, NJ, 1992.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1993.

[Sil00] Joseph H. Silverman. On the distribution of integer points on curves of genus zero. *Theoret. Comput. Sci.*, 235(1):163–170, 2000. Selected papers in honor of Manuel Blum (Hong Kong, 1998).

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Sur00] David B. Surowski. The snake lemma in an abelian category with enough projectives (injectives). *Comm. Algebra*, 28(1):249–253, 2000.

[Tat74] John T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.